Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A security system for securing data in a computer network comprising:

a plurality of user terminals coupled to the computer network;

a plurality of cryptographic devices remote from the plurality of user terminals and coupled to the computer network, wherein each cryptographic device includes a computer executable code for authenticating one or more users and verifying that the authenticated user is authorized to assume a role, and wherein each cryptographic device is capable of performing value management functions for one or more users; and

a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user,

wherein each cryptographic device is not dedicated to particular user terminals, and

wherein each cryptographic module is programmable to service any of the plurality of user terminals.

2. (Previously Presented) The system of claim 1, wherein the security device transaction data related to a user is loaded into one of the plurality of cryptographic devices when the user requests to operate on a value bearing item.

3. (Original) The system of claim 1, wherein the assumed role includes one or more corresponding operations to be performed by the authenticated user.

4. (Original) The system of claim 1, wherein the assumed role is a security officer role to initiate a key management function.

5. (Original) The system of claim 1, wherein the assumed role is a key custodian role to take possession of shares of keys.

6. (Original) The system of claim 1, wherein the assumed role is an administrator role to manage a user access control database.

7. (Original) The system of claim 1, wherein the assumed role is an auditor role to manage audit logs.

8. (Original) The system of claim 1, wherein the assumed role is a provider role to withdraw from a user account.

9. (Original) The system of claim 1, wherein the assumed role is a user role to operate on a VBI.

10. (Original) The system of claim 1, wherein the assumed role is a certificate authority role to allow a public key certificate to be loaded and verified.

11. (Previously Presented) The system of claim 1, wherein each cryptographic device includes a state machine for determining a state corresponding to availability of one or more commands in conjunction with the role.

12. (Previously Presented) The system of claim 1, wherein each cryptographic device is stateless.

13. (Previously Presented) The system of claim 1, wherein each cryptographic device includes a computer executable code for preventing unauthorized modification of data.

14. (Previously Presented) The system of claim 1, wherein each cryptographic device includes a computer executable code for ensuring the proper operation of cryptographic security and VBI related meter functions.

15. (Original) The system of claim 1, wherein at least one of the user is an enterprise account.

16. (Previously Presented) The system of claim 1, wherein each cryptographic device includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

17. (Original) The system of claim 2, wherein the value bearing item is a mail piece.

18. (Previously Presented) The system of claim 17, wherein the mail piece comprises a digital signature.

19. (Previously Presented) The system of claim 1, wherein one of the plurality of cryptographic devices encrypts validation information according to a user request for printing a VBI.

20. (Previously Presented) The system of claim 17, wherein one of the plurality of cryptographic devices generates data sufficient to print a postal indicium in compliance with postal service regulation on the mail piece.

21. (Original) The system of claim 2, wherein the value bearing item is a ticket.

22. (Original) The system of claim 2, wherein a bar code is printed on the value bearing item.

23. (Original) The system of claim 1, wherein each security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code. a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

24. (Original) The system of claim 1, wherein each security device transaction data includes a private key, a public key, and a public key certificate, wherein the private key is used to sign device status responses and a VBI which, in conjunction with a public key certificate, demonstrates that the device and the VBI are authentic.

25. (Original) The system of claim 1 further comprising at least one more cryptographic device remote from the plurality of user terminals coupled to the computer network, wherein the at least one more cryptographic device includes a computer executable code for authenticating any of the plurality of users.

26. (Previously Presented) The system of claim 25, wherein one of the plurality of cryptographic devices shares a secret with the at least one more cryptographic device.

27. (Original) The system of claim 25, wherein one of the plurality of cryptographic devices is a master device and generates a master key set (MKS).

28. (Original) The system of claim 27, wherein the MKS includes a Master Encryption Key (MEK) used to encrypt keys when stored outside the device and a Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device.

29. (Original) The system of claim 27, wherein the MKS is exported to other cryptographic devices by any cryptographic device.

30. - 68. (Cancelled)